Attorney Docket No. B-4278 619005-7 *PATENT*

AF

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant: Liqun Chen	)	On Appeal to the
	)	Board of Appeals
Patent Application No.: 09/913,454	)	
	)	Group Art Unit: 2137
Filed: 08/14/2001	)	
	)	Examiner: Nguyen, Minh Dieu T
	)	
For: "Protection of the Configuration ..."	)	
	)	Date: January 5, 2007
	)	

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the Final rejection, dated July 18, 2006, for the above identified patent application. Appellant submits that this Appeal Brief is being timely filed, since the Notice of Appeal was filed on November 8, 2006. Please charge the Appeal Brief fee of $500.00 to deposit account no. 08-2025.

REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC

RELATED APPEALS AND INTERFERENCES

Appellant submits that there are no other prior and pending appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1-64 are currently pending. Claims 1-43 have been canceled without prejudice and Claims 44-64 are the subject of this Appeal and are reproduced in the accompanying Claims appendix.

STATUS OF AMENDMENTS

No Amendment After Final Rejection has been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

The invention described and claimed in the present application relates to the protection of configuration of modules in a computing apparatus (p. 1, ll. 3-4).

Claim 44 of the present disclosure is directed to a method of protecting from modification computer apparatus (10) comprising a plurality of functional modules (15), wherein the computer apparatus contains or is in communication with a trusted device (24) adapted to respond to a user in a trusted manner, the method comprising: storing a module configuration of the computer apparatus providing an identification of each functional module in the computer apparatus; the trusted device performing a cryptographic identification process for modules with a cryptographic identity to identify them and thereby determine an actual module configuration (Fig. 4, p. 11, l. 1 to p. 13, l. 8); the trusted device comparing the actual module configuration against the stored module configuration; and the trusted device inhibiting function of the computer apparatus while the actual module configuration does not satisfactorily match the stored module configuration (Fig. 5, p. 13, l. 26 to p. 15).

Claim 52 of the present disclosure is directed to a computer apparatus (10) adapted for protection against modification, the computer apparatus comprising a plurality of functional modules (15), one of said modules being a trusted device (24) adapted to respond to a user in a trusted manner, the computer apparatus having a module configuration providing an identification of each functional module in the computer apparatus, wherein the trusted device is adapted to compare a module configuration of the computer apparatus against a stored module configuration by performing a cryptographic identification process for modules with a cryptographic identity to determine an actual module configuration and to compare the actual module configuration against the stored module configuration (Fig. 5, p. 13, l. 26 to p. 15).

Claim 54 of the present disclosure is directed to a security token (19) adapted to hold a stored module configuration of modules in a computer apparatus, the stored module configuration providing an identification of each functional module in the computer apparatus as validly formed, and adapted to provide the stored module configuration to the computer apparatus to allow comparison between an actual module configuration of the computer apparatus and the stored module configuration (Fig. 6, p. 16, l. 1 to p.18, l. 4).

Claim 57 of the present disclosure is directed to a method of protecting from modification computer apparatus (10) comprising a plurality of functional modules (15) by monitoring the configuration of functional modules within the computer apparatus, the method comprising: storing a module configuration of the computer apparatus, the module configuration being an identification of each functional module in the computer apparatus as validly formed, on a security token removably attachable to the computer apparatus; and checking an actual module configuration against the stored module configuration, and inhibiting function of the computer apparatus if the actual module

configuration does not satisfactorily match the stored module configuration (Figs 4-6, p. 13, l. 26 to p. 15, p. 16, l. 1 to p.18, l. 4).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1: Whether Claims 44-47, 50, 52-53 and 58 are patentable under 35 U.S.C. 103(a) in view of Drews, U.S. Patent No. 6,539,480, (hereinafter "Drews") and further in view of Selitrennikoff, U.S. Patent No. 6,209,089, (hereinafter "Selitrennikoff")?

Issue 2: Whether Claims 54-56 are patentable under 35 U.S.C. 103(a) in view of Herzi, U.S. Patent No. 6,353,885, (hereinafter "Herzi") and further in view of Selitrennikoff, U.S. Patent No. 6,209,089, (hereinafter "Selitrennikoff")?

Issue 3: Whether Claims 48-49, 57, 59 and 60-63 are patentable under 35 U.S.C. 103(a) in view of Drews, Selitrennikoff and further in view of Herzi, U.S. Patent No. 6,353,885, (hereinafter "Herzi")?

Issue 4: Whether Claims 51 and 64 are patentable under 35 U.S.C. 103(a) in view of Drews, Selitrennikoff, Herzi and further in view of Muftic, U.S. Patent No. 5,943,423, (hereinafter "Muftic")?

ARGUMENT

Issue 1: Whether Claims 44-47, 50, 52-53 and 58 are patentable under 35 U.S.C. 103(a) in view of Drews and further in view of Selitrennikoff?

In the final Office Action of July 18, 2006, the Examiner rejects Claims 44-47, 50, 52-53 and 58 under 35 U.S.C. 103(a) as being obvious in view of Drews and Selitrennikoff. Appellant respectfully disagrees.

I. Appellant submits that a *prima facie* case of obviousness has **not** been established because the Examiner has failed to show that Drews and Selitrennikoff teach each and every element as claimed in the present application. In particular:

Claim 44

A. Appellant submits that the Examiner has not shown that Drews and Selitrennikoff disclose, suggest or teach, *inter alia*, the following features recited by Claim 44 of the present application:

> "**storing a module configuration** of the computer apparatus ... the trusted device **comparing** the **actual module configuration against the stored module configuration**" (emphases added)

The Examiner asserts that this feature is disclosed by Drews' trusted authority information "45" (p. 3, section 6). The Examiner also asserts that the feature of "the trusted device comparing the actual module configuration against the stored module configuration" as recited in Claim 44 is disclosed by Drews' Figure 3, step "117" and Drews' Figure 5 , step "207" (p. 2, section 4). Appellant respectfully traverses the Examiner's assertions.

According to Drews, Figure 3's element "117" is illustrated in detail in Drews' Figure 5 reproduced below and described in column 6, lines 1-19 of Drews.

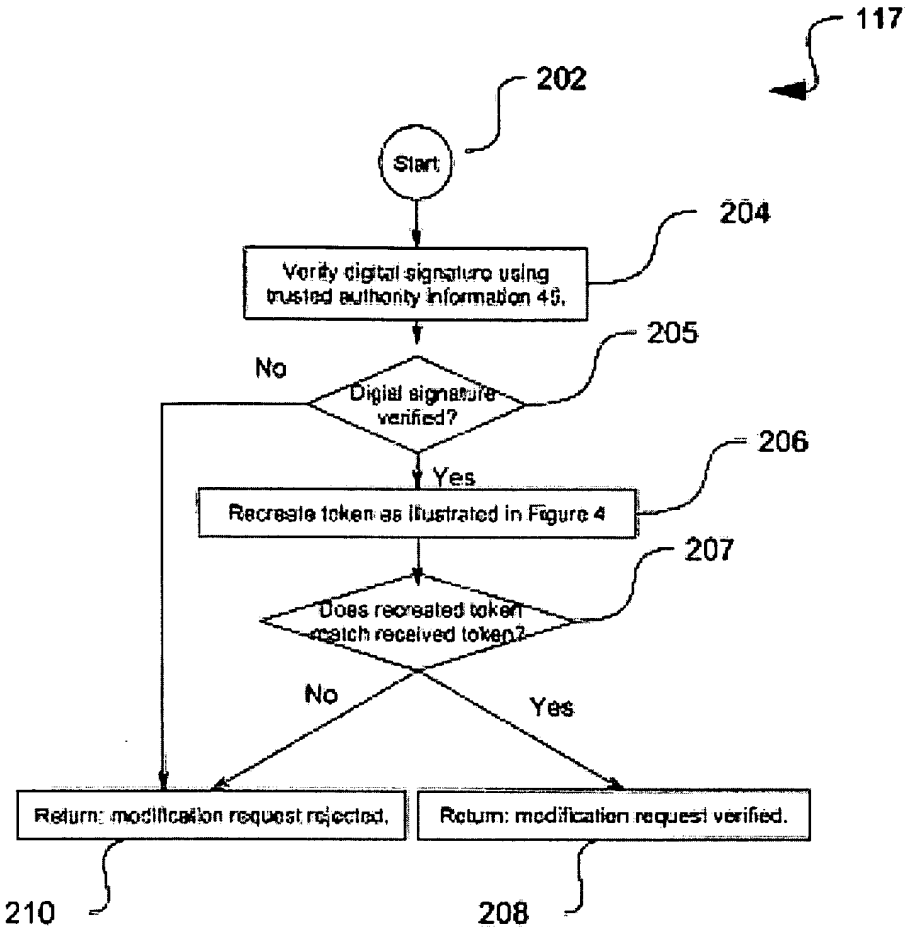


Figure 5

According to Figure 5 above, in step "207," referred to by the Examiner, Drews' security module "30" compares a temporary token with a token received in a modification request. See column 6, lines 13-15 of Drews. The Examiner appears to allege that comparing a temporary token with a token received in the modification request discloses "comparing the actual module configuration against the stored module configuration" as recited in Claim 44. The Examiner's assertion wrongfully implies that one of Drews' tokens reads on the "actual module configuration" as recited in Claim 44 and the other token reads on the "stored module configuration" as recited in Claim 44.

Appellant respectfully submits that neither the temporary token nor the token received in the modification request reads upon the "stored module configuration" as recited in Claim 44 because neither one is described anywhere in Drews as being stored.

According to Drews, one of the tokens being compared in the step 207 is recreated in Drews's step 206, shown above in Figure 5, and the other token being compared in the step 207 is created in Drews' step 113. Both of Drews's token creating steps 206 and 113 use the process of Figure 4, reproduced below, to create their respective tokens.

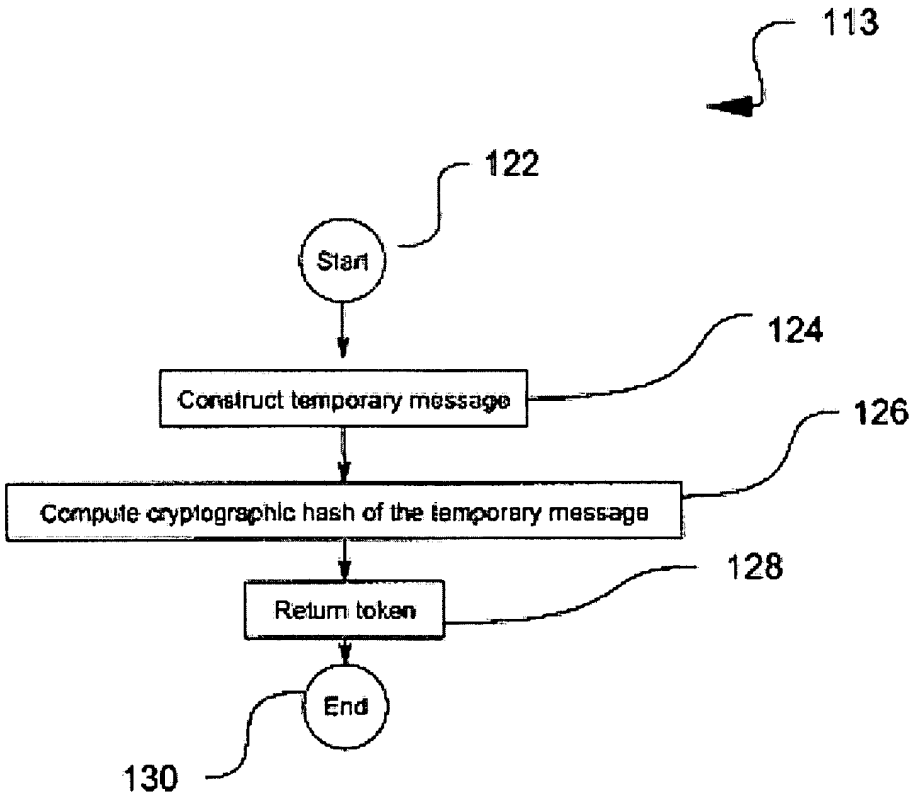


Figure 4

According to Drews' Figure 4 above, the tokens are created, but **not** stored. Contrary to Drews, the "module configuration" recited in Claim 44 is being **stored** and the **stored**

"module configuration" is being compared to the "actual module configuration" recited in Claim 44.

Although the Examiner alleges that Drews' trusted authority information "45" discloses "storing a module configuration" as recited in Claim 44, Appellant submits that Drews does not teach, disclose or suggest storing any tokens in the trusted authority information "45" and the Examiner failed to comply with 37 C.F.R. §1.104(c)(2) and "designate as nearly as practicable" where Drews discloses storing tokens in the trusted authority information "45."

Because Drews does not store tokens, the step 207 does not disclose "comparing the actual module configuration against the **stored** module configuration" (emphasis added) as recited in Claim 44. Hence, Claim 44 is patentable over Drews and Selitrennikoff and the rejection should be overturned on appeal.

B. Appellant submits that the Examiner has not shown that Drews and Selitrennikoff disclose, suggest or teach, *inter alia*, the following features recited by Claim 44 of the present application:

> "the trusted device **inhibiting function of the computer apparatus** while the actual module configuration does not satisfactorily match the stored module configuration" (emphasis added)

The Examiner asserts that this feature is disclosed by Drews' elements "210" (p. 3, section 6). Appellant respectfully traverses the Examiner's assertion.

According to Drews, a security module "30" is able to validate a modification request to configure computer "10." See column 6, lines 1-3, element 117 and Figure 5 of Drews. During the validation process, as shown in Drews' Figure 5 above, the security module

"30"simply **rejects** the modification request by going to element "210" when the created token does not match the received token in step 207 without any further action.

Because the security module "30" only **rejects the modification request** in element "210," Drews does not teach, disclose or suggest that the security module "30" is able to **inhibit** function of the computer "10."

In responding to Appellant's arguments, the Examiner alleges that when new or modified configuration data is rejected, the computer stops operating under the new/modified/actual configuration data (p. 2, section 4). How can the computer **stop** operating under the new/modified/actual configuration data, as alleged by the Examiner, when the computer never operated under the new/modified/actual configuration data to begin with? The Examiner offers no support for this bold assertion which, with all due respect, does not even make sense.

Appellant respectfully maintains that, contrary to the Examiner's assertions, there is no teaching or suggestion in Drews that the security module "30" is able to **inhibit** function of the computer "10." Hence, Claim 44 is patentable over Drews and Selitrennikoff and the rejection should be overturned on appeal.

Claims 45-47 and 50

Claims 45-47 and 50, at least based on their dependency on Claim 44, are also patentable over Drews and Selitrennikoff and the rejection should be overturned on appeal..

Claim 52

Appellant submits that, at least for the reasons stated above for Claim 44, Drews and Selitrennikoff do not teach, disclose or suggest "trusted device is adapted to **compare** a module configuration of the computer apparatus against a **stored module configuration** by performing a cryptographic identification process for modules with a

cryptographic identity to determine an actual module configuration" (emphasis added) as recited in Claim 52. Hence, Claim 52 is patentable over Drews and Selitrennikoff and should be allowed by the Examiner. Claim 53, at least based on its dependency on Claim 44, is also believed to be patentable over Drews and Selitrennikoff and the rejection should be overturned on appeal.

Claim 58

The Examiner rejects dependent Claim 58 in view of Drews and Selitrennikoff. Appellant respectfully note that Claim 58 depends from Claim 54 which is not rejected in view of Drews and Selitrennikoff, and submits that Claim 58 is therefore implicitly patentable over Drews and Selitrennikoff as well.

II. Appellant further submits that a *prima facie* case of obviousness has **not** been established because there is no motivation in the prior art to combine the cited references as asserted by the Examiner. In particular:

Appellant respectfully submits that there is no suggestion or motivation on the face of either Drews or Selitrennikoff for their combination nor any teaching as to how the features of the two devices could be combined so as to meet the structure as claimed in the present application. It has been found that "when the incentive to combine the teachings of the references is not readily apparent, it is the duty of the examiner to explain why combination of the teachings is proper. ... Absent such reasons or incentives, the teachings of the references are not combinable" Ex parte Skinner, 2 USPQ2d 1788 (B.P.A.I. 1986). Appellant submits that the Examiner's combination of Drews and Selitrennikoff is based upon a hindsight reconstruction of Appellant's claims as opposed to what the references really suggest.

Drews relates to the use of a security module in computer apparatus to validate

requests to reconfigure the computer system. Configuration data, in the terms of Drews, primarily relates to software used to boot the system, but can also relate to other software (column 3, ll. 23-41), but there is no suggestion in Drews that it can cover anything other than software. Drews relates to a process for changing configuration data - this can be achieved by use of a digital signature to ensure that the request for a change comes with the proper authority. This is achieved by using configuration data (in the sense of Drews) digitally signed by a trusted party.

Appellant submits that nothing in Drews teaches identification of functional modules within a computing apparatus. Therefore there appears to be no motivation in Drews to consider such a thing, as this falls outside the discussion of "configuration" identified above. The concern of Drews appears to be to ensure that the software environment of a computer platform is not changed unless a request is received which has the authority of a trusted party. Any request which does not have this authority is simply not effective. Modification or substitution of hardware or any other specific functional modules appears outside the contemplation of Drews.

It is not apparent why the reader of Drews would seek to use any teaching from Seletrennikoff. Seletrennikoff relates to booting computers using a client-server connection in such a way that the boot will not be adversely affected by changes in the hardware configuration of the computers. Although Seletrennikoff teaches that values associated with certain hardware components of the computer be stored in a configuration file and that this configuration file is compared with the actual values of the values, Seletrennikoff's actual values are detected by the client computer itself, and the configuration file is held remotely on the server. Seletrennikoff does **not** appear to relate to providing protection against modification of the computer - merely to ensuring that booting over the network is still achievable - and therefore itself neither teaches nor suggests the invention. The result of a mismatch between detected and stored information is to download further operating system components from the server to the

client computer - any mismatch results directly in modification of the client operating system (see Abstract of Seletrennikoff). Moreover, as there is no suggestion in Seletrennikoff that it has any bearing on protection against unauthorized modification of a computer apparatus, or to provide a permission process for modification of a computer apparatus, it is not remotely clear why a person skilled in the art starting from Drews would seek to use any teaching from Seletrennikoff.

Appellant submits that one skilled in the art would not find any suggestion or motivation in the cited references as a whole to combine or modify the two devices disclosed in the cited references to meet the structure as claimed in the present application.

Issue 2: Whether Claims 54-56 are patentable under 35 U.S.C. 103(a) in view of Herzi and further in view of Selitrennikoff?

In the final Office Action of July 18, 2006, the Examiner rejects Claims 54-56 under 35 U.S.C. 103(a) as being obvious in view of Herzi and Selitrennikoff. Appellant respectfully disagrees.

Appellant submits that a *prima facie* case of obviousness has not been established because the Examiner has failed to show that Herzi and Selitrennikoff teach each and every element as claimed in the present application. In particular:

Claim 54

Appellant submits that the Examiner has not shown that Herzi and Selitrennikoff disclose, suggest or teach, *inter alia*, the following features recited by Claim 54 of the present application:

> "adapted to provide the stored module configuration to the computer apparatus to allow **comparison between an actual module configuration**

of the computer apparatus and the stored module configuration"
(emphasis added)

The Examiner asserts that this feature is disclosed by Herzi's elements "78" (p. 5, ll. 1-2). The Examiner also asserts that the "stored module configuration" as recited in Claim 54 is disclosed by Herzi's BIOS level settings stored on Herzi's smart card "28" (p. 4, section 7a).

However, Appellant respectfully submits that the Examiner failed to comply with 37 C.F.R. §1.104(c)(2) and "designate as nearly as practicable" where Herzi discloses "an actual module configuration" as recited in Claim 54. The Examiner attempts to show that Herzi's element "78" compares the "actual module configuration" and the "stored module configuration" as recited in Claim 54 without any showing where Herzi discloses the "actual module configuration." Appellant submits that Herzi does not disclose the "actual module configuration" as recited in Claim 54.

According to Herzi, element "78" determines whether or not a change has occurred in the BIOS level settings. See column 7, lines 12-14 of Herzi. However, Herzi is silent as to **what** is being compared to determine whether or not a change has occurred in the BIOS level settings. Appellant submits that Herzi does not teach, disclose or suggest comparing "between an actual module configuration of the computer apparatus and the stored module configuration" as recited in Claim 54, because Herzi does not disclose the "actual module configuration" as recited in Claim 54.

Hence, Claim 54 is patentable over Herzi and Selitrennikoff and the rejection should be overturned on appeal.

Claims 55-56

Claims 55-56, at least based on their dependency on Claim 54, are also patentable over Herzi and Selitrennikoff and the rejection should be overturned on appeal..

Issue 3: Whether Claims 48-49, 57, 59 and 60-63 are patentable under 35 U.S.C. 103(a) in view of Drews, Selitrennikoff and further in view of Herzi?

In the final Office Action of July 18, 2006, the Examiner rejects Claims 48-49, 57, 59 and 60-63 under 35 U.S.C. 103(a) as being obvious in view of Drews, Selitrennikoff and Herzi. Appellant respectfully disagrees.

Appellant submits that a *prima facie* case of obviousness has not been established because the Examiner has failed to show that Drews, Selitrennikoff and Herzi teach each and every element as claimed in the present application. In particular:

Claims 48-49

Appellant submits that Claims 48-49, at least based on their dependency on Claim 44, are believed to be patentable over Drews, Selitrennikoff and Herzi, because there is no prima facie 35 USC 103(a) case based on Drews and Selitrennikoff, as shown above, and because the Examiner has not shown where Herzi discloses, teaches or suggests the features not found in Drews and Selitrennikoff.

Claim 57

Appellant submits that, at least for the reasons stated above for Claims 44 and 54, Drews, Selitrennikoff and Herzi do not teach, disclose or suggest "checking an actual module configuration **against the stored module configuration**" (emphasis added) and "**inhibiting** function of the computer apparatus if the actual module configuration does not satisfactorily match the stored module configuration" (emphasis added) as recited in Claim 57. Hence, Claim 57 is patentable over Drews, Selitrennikoff and Herzi and the rejection should be overturned on appeal.

Claims 59 and 60-63

Claims 59 and 60-63, at least based on their dependency on Claim 57, are also patentable over Drews, Selitrennikoff and Herzi and the rejection should be overturned on appeal.

Issue 4: Whether Claims 51 and 64 are patentable under 35 U.S.C. 103(a) in view of Drews, Selitrennikoff, Herzi and further in view of Muftic?

In the final Office Action of July 18, 2006, the Examiner rejects Claims 51 and 64 under 35 U.S.C. 103(a) as being obvious in view of Drews, Selitrennikoff, Herzi and Muftic. Appellant respectfully disagrees.

Claims 51 and 64

Appellant submits that Claims 51 and 64, at least based on their dependency on Claims 44 and 57, respectively, are believed to be patentable over Drews, Selitrennikoff, Herzi and Muftic, because there is no prima facie 35 USC 103(a) case based on Drews and Selitrennikoff, as shown above, and because the Examiner has not shown where Herzi and Muftic disclose, teach or suggest the features not found in Drews and Selitrennikoff.

* * *

Conclusion

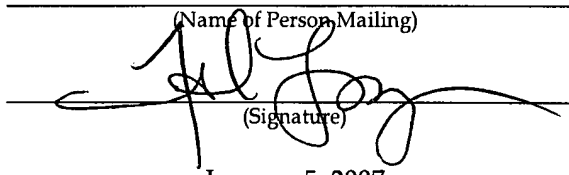
For the extensive reasons advanced above, Appellant respectfully contends that each claim is patentable. Therefore, reversal of all rejections and objections is courteously solicited.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this Appeal Brief is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is being deposited with the United States Post Office with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22323-1450 on

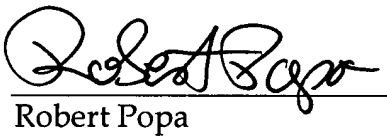
January 5, 2007
(Date of Mailing)

Trisha Lozano
(Name of Person Mailing)


(Signature)

January 5, 2007
(Date)

Respectfully submitted,



Robert Popa
Attorney for Appellants
Reg. No. 43,010
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300

Encl.:
Claims appendix;
Evidence appendix;
Related Proceedings appendix;
Postcard.

1-43. (cancelled)

44. A method of protecting from modification computer apparatus comprising a plurality of functional modules, wherein the computer apparatus contains or is in communication with a trusted device adapted to respond to a user in a trusted manner, the method comprising:

storing a module configuration of the computer apparatus providing an identification of each functional module in the computer apparatus;

the trusted device performing a cryptographic identification process for modules with a cryptographic identity to identify them and thereby determine an actual module configuration;

the trusted device comparing the actual module configuration against the stored module configuration; and

the trusted device inhibiting function of the computer apparatus while the actual module configuration does not satisfactorily match the stored module configuration.

45. A method as claimed in claim 44, wherein the stored module configuration is held separately from the computing apparatus.

46. A method as claimed in claim 44, wherein the stored module configuration is stored such that it is accessible only by a cryptographic authentication process.

47. A method as claimed in claim 44, wherein the trusted device is adapted to communicate securely with the stored module configuration.

48. A method as claimed in claim 47, wherein the stored module configuration is stored in a security token.

49. A method as claimed in claim 48, wherein the security token is a smart card.

50. A method as claimed in claim 44, wherein the step of checking of the actual module configuration comprises a cryptographic identification process for modules with a cryptographic identity.

51. A method as claimed in claim 48, wherein a stored module configuration is held by a remote module validation authority and the remote validation authority provides a service allowing a replacement security token to be provided if a security token is lost or stolen.

52. Computer apparatus adapted for protection against modification, the computer apparatus comprising a plurality of functional modules, one of said modules being a trusted device adapted to respond to a user in a trusted manner, the computer apparatus having a module configuration providing an identification of each functional module in the computer apparatus, wherein the trusted device is adapted to compare a module configuration of the computer apparatus against a stored module configuration by performing a cryptographic identification process for modules with a cryptographic identity to determine an actual module configuration and to compare the actual module configuration against the stored module configuration.

53. Computer apparatus as claimed in claim 52, wherein the stored module configuration is held separately from the computing apparatus and wherein the computer apparatus is adapted to obtain the stored module configuration by a cryptographic authentication process.

54. A security token adapted to hold a stored module configuration of modules in a computer apparatus, the stored module configuration providing an identification

of each functional module in the computer apparatus as validly formed, and adapted to provide the stored module configuration to the computer apparatus to allow comparison between an actual module configuration of the computer apparatus and the stored module configuration.

55. A security token as claimed in claim 54, wherein the stored module configuration is stored in an encrypted form.

56. A security token as claimed in claim 54, wherein the security token is a smart card.

57. A method of protecting from modification computer apparatus comprising a plurality of functional modules by monitoring the configuration of functional modules within the computer apparatus, the method comprising:

storing a module configuration of the computer apparatus, the module configuration being an identification of each functional module in the computer apparatus as validly formed, on a security token removably attachable to the computer apparatus; and

checking an actual module configuration against the stored module configuration, and inhibiting function of the computer apparatus if the actual module configuration does not satisfactorily match the stored module configuration.

58. A method as claimed in claim 57, wherein the stored module configuration is stored such that it is accessible only by a cryptographic authentication process.

59. A method as claimed in claim 58, wherein the computer apparatus contains or is in communication with a trusted device adapted to respond to a user in a trusted manner and the trusted device is adapted to perform the step of checking the actual module configuration against the stored module configuration.

60. A method as claimed in claim 59, wherein the trusted device is adapted to communicate securely with the security token.

61. A method as claimed in claim 57, wherein the security token is a smart card.

62. A method as claimed in claim 57, wherein the stored module configuration is also held by a remote module validation authority.

63. A method as claimed in claim 62, wherein the step of checking the actual module configuration against the stored module configuration involves use of the stored module configuration held by the remote module validation authority.

64. A method as claimed in claim 62, wherein the remote validation authority provides a service allowing a replacement security token to be provided if a security token is lost or stolen.

No evidence is being submitted

No copies of decisions rendered in related proceedings are being submitted.